UNITED STATES PATENT APPLICATION

FOR

PORT ISOLATION FOR RESTRICTING TRAFFIC FLOW ON LAYER 2 SWITCHES

INVENTORS:

MONICA JOSHI, a citizen of India
PAULINE SHUEN, a citizen of the United States of America

ASSIGNED TO:

CISCO TECHNOLOGY, INC., a California Corporation

Attorney Docket Number: CISCO-2828

Client Docket Number: 2828

PREPARED BY:

D'ALESSANDRO & RITCHIE
P.O. BOX 640640
SAN JOSE, CA 95164-0640
TELEPHONE: (408) 441-1100
FAX: (408) 441-8400

SPECIFICATION

TITLE OF INVENTION

PORT ISOLATION FOR RESTRICTING TRAFFIC FLOW ON LAYER 2 SWITCHES

FIELD OF THE INVENTION

The present invention relates to layer 2 switches. More particularly, the present invention relates to a method an apparatus to isolate ports on layer 2 switches to restrict traffic flow.

BACKGROUND OF THE INVENTION

Modern computer networks are divided up into layers. Each layer is responsible for providing some service to the layer above it, and may use the services of the layer below it. The International Standards Organization ("ISO") defined seven layers as a standard for computer networks. The layers are defined as follows:

1. A physical layer, which is responsible for transmitting unstructured bits of information across a link;

2. A data link layer, which transmits chunks of information across a link. It handles error notification, network topology, and flow control. Ethernet, Token Ring, and FDDI are media access methods that offer the functionality defined by the data link layer;

3. A network layer, which is responsible for ensuring that any pair of systems in the network can communicate with each other;

4. A transport layer, which establishes a reliable communications stream between a pair of systems;

5. A session layer, which offers services above the simple full-duplex reliable communication stream provided by the transport layer;

6. A presentation layer, which is responsible for providing a means by which applications can agree on representations of data; and

7. An application layer, which runs applications.

This invention relates only to layer 2, the data link layer or the MAC layer. Layer 2 is the communication protocol which contains the physical address of a client or server station which is inspected by a bridge or switch. The layer 2 switch then forwards traffic based on the MAC layer (Ethernet or Token Ring) addresses. Currently, traffic flows such as such as broadcast, unknown multicast, or unknown unicast received at the switch are not isolated between ports on the switch so that every user on the same virtual local area network (VLAN) is able to see the traffic generated by another user on the same

VLAN. There are currently many users, such as multi-dwelling unit or multi-tenant unit users which obtain network connectivity through layer 2 switches, which have confidentiality and security concerns and would like to prevent others from seeing their traffic.

Currently, one way to achieve complete isolation between access ports at layer 2 is to assign each user port an individual VLAN. The disadvantage of this approach is that the number of VLANs can grow considerably large as the number of user ports increase. This is also not a practical solution where a large number of switches are connected to each other as well as providing connections to home users, thereby increasing the number of VLANs dramatically. Thus, there exists a need for access port isolation that is more efficient and would allow port isolation at a layer 2 switch that belongs to the same VLAN.

SUMMARY OF THE INVENTION

This invention provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map which is responsive to a destination address of an incoming packet.

The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on an data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or nonprotected port.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this Specification, illustrate one or more embodiments of the invention and, together with the present description, serve to explain the principles of the invention.

In the drawings:

FIG. 1 is a diagram of a specific embodiment of the present invention.

FIG. 2 is a flow chart showing a specific embodiment of the present invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

An embodiment of the present invention is described herein in the context of layer 2 switches. Those of ordinary skill in the art will realize that the following description of the present invention is illustrative only and not in any way limiting. Other embodiments of the invention will readily suggest themselves to such skilled persons having the benefit of this disclosure. Reference will now be made in detail to implementations of the present invention as illustrated in the accompanying drawings. The same reference numbers will be used throughout the drawings and the following description to refer to the same or like parts.

In the interest of clarity, not all the routine features of the implementations described herein are described. It will of course be appreciated that in the development of any such actual implementation, numerous implementation-specific decisions must be made to achieve a developer's specific goals, such as compliance with system- and business-related constraints, and that these goals will vary from one implementation to another. Moreover, it will be appreciated that such a development effort might be complex and time-consuming, but would nevertheless be a routine undertaking of engineering for those of ordinary skill in the art having the benefit of this disclosure.

In accordance with the present invention, the components, process steps, and/or data structures may be implemented using various types of operating systems, computing platforms, computer programs, and/or general purpose machines. In addition, those of ordinary skill in the art will recognize that devices of a less general purpose nature, such

as hardwired devices, field programmable gate arrays (FPGAs), application specific integrated circuits (ASICs), or the like, may also be used without departing from the scope and spirit of the inventive concepts disclosed herein.

Ethernet is the most widely-used local area network ("LAN") and is normally a shared media LAN. All stations on the segment share the total bandwidth, which is currently either 10 Mbps, 100 Mbps, or 1000 Mbps. With the increase in security concerns, the multiple traffic flows received at a switch need to be isolated within each port on layer 2 switches 12. The traffic may be broadcast traffic, where the data packet(s) 10 is transmitted to everyone on the network, unknown or known unicast, where the data packet(s) 10 is transmitted from one station to another such as from a client to a server or from a server to another server, or multicast, where the data packet(s) 10 is transmitted to a predetermined list of recipients.

Referring to FIG. 1, ports on a layer 2 switch 12 may be isolated by a user by using a port configurer 11, such as a Command Line Interface (CLI) to configure a port as a protected port or a non-protected port. The ports may be configured from a port configurer 11 through programming or network management. Once a data packet 10 is received by the layer 2 switch 12, a forwarding map generator 14 generates a forwarding map to direct the data packet 10 to its respective ports, however, the global mask 18 on the layer 2 switch 12 may edit the forwarding feature of the data packet 10 depending on whether the ingress or source port 22 is a protected port or non-protected port. The global mask 18 acts as an editor to change the forwarding features of the data packet 10

by modifying/changing the port numbers on the forwarding map. If the ingress port 22 is configured to be a protected port, the data packet 10 received by that port will not be forwarded to any other protected ports 26 on the switch, but may be forwarded to other non-protected ports 24. Thus, the global mask 18 will modify the forwarding map so that the data packet will not be forwarded to ports configured as protected ports 26. If, on the other hand, the ingress port 22 is a non-protected port, the data packet 10 received by that port can be forwarded to all other ports whether configured as protected 26 or non-protected 24. Once the data packet 10 is sent to all ports as directed by the forwarding map 14, it may then be directed to an uplink 28 and onto a router or a network 30. However, those skilled in the art will realize that the uplink 28 and router/network 30 are not necessary to carry out the present invention.

The forwarding map is generated by a forwarding map generator 14. The forwarding map generator 14 looks to an address table 16, which has a list of destination addresses matched with a port number, to match the destination address on the data packet 10 with a port number. Whether or not a match is found, if the ingress port 22 is a non-protected port 22, the forwarding map 14 will direct the data packet 10 to all other ports on the switch 12 whether it is a non-protected 24 or protected port 26. However, if the ingress port 22 is a protected port, the global mask 18 will adjust the forwarding map 14 so that only non-protected ports 24 may receive the data packet 10 and not other protected ports 26.

Now referring to FIG. 2, the present invention also provides for a method for isolating ports on a layer 2 switch. The ports are configured as protected or non-protected ports by a user 40. A data packet is received by a layer 2 switch 42 which generates a forwarding map for the data packet 48. The destination address on the data packet is matched with a physical address or port number on the layer 2 switch by looking to an address table 46. Whether or not a match is found, ifhe ingress port is a protected port 50, the global mask will edit the forwarding map so that the data packet is sent to all other non-protected ports only and not any of the other protected ports 52. However, if the ingress port is a non-protected port 50, then all ports, whether non-protected or protected may receive the data packet 54. Once the data packet is sent to all necessary ports as directed by the forwarding map, the data packet may be sent to an uplink and onto a router or network. However, those skilled in the art will realize that the uplink and router/network are not necessary to carry out the present invention.

While embodiments, examples, and applications of this invention are shown and described, it would be apparent to those of ordinary skill in the art having the benefit of this disclosure that many more modifications than mentioned above are possible without departing from the inventive concepts herein. Thus, what has been disclosed is merely illustrative of the present invention and other arrangements or methods can be implemented by those skilled in the art without departing from the spirit and scope of the present invention.